UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/587,932	06/06/2000	Xin Qiu	D02308	8876

43471 7590 01/19/2007		EXAMINER	
GENERAL INSTRUMENT CORPORATION DBA THE CONNECTED HOME SOLUTIONS BUSINESS OF MOTOROLA, INC. 101 TOURNAMENT DRIVE HORSHAM, PA 19044		SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	09/587,932	QIU ET AL.
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-9,14-17 and 23-26* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 6-9, 14-17, and 23-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This Office Action is responding to the After Final received on 12/14/06.

2.   Claims 1-4, 6-9, 14-17, and 23-26 are pending.

Response to Arguments

3.   Applicant's arguments, see After Final, filed 12/14/06, with respect to the

rejection(s) of claim(s) 1-4, 6-9, 14-17, and 23-26 under 102(3) and 103(a)

rejection basis have been fully considered and are persuasive. Therefore, the

rejection has been withdrawn. However, upon further consideration, a new

ground(s) of rejection is made in view of Wasilewski and Milsted.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5.   Claims 1-3, 7-9, 14-17, and 24-26 are rejected under 35 U.S.C. 102(b) as being

anticipated by Wasilewski et al, PCT Publication No. WO 94/10775.

6.   As per claims 1 and 24:

Wasilewski discloses "A method of providing data, the method comprising:

storing a first set of encryption data associated with a first data stream wherein the first

data stream includes a first number of services" on (Page 25 lines 32-35) {Video, and

multiplexed Audio services};

encrypting the first data stream having a first-level-of-encryption" on (Page 26

lines 1-10);

sending the first data stream to a destination device for decryption" on (Set-top

decoder 260, Page 34 lines 23-32);

"storing a second set of encryption data associated with a second data stream

wherein the second data stream includes a second number of services that is different

from the first number of services" on (Page 22 line 26 to Page 23 line14, and Page 26

lines 1-10) {The seeds used to encrypt the number of services are changed every

cryptocycle. Since new seeds created for encryption of new number of services, the

first level of encryption is different from the second level of encryption. (See Page 23

lines 1-15)};

encrypting the second data stream having a second-level-of-encryption, the

first-level-of-encryption being different from the second-level-of-encryption" on (Page 26

lines 1-10)

"utilizing a common memory to encrypt said the first data stream at first-level of

encryption and to encrypt the second data stream at the second-level-of encryption" on

(page 26, Global encrypter 128); and

sending the second data stream to the destination device for decryption" on

(Set-top decoder 260, Page 34 lines 23-32).

7. As per claims 2 and 25:

Wasilewski discloses "The method of claim 1 wherein the first set of encryption data

comprises at least one encryption key" on (Page 26 lines 1-10).

8. As per claim 3:

Wasilewski does discloses "The method of claim 1 wherein the destination device

comprises a set-top box" on (Page 30 line 3, and Fig 15).

9. As per claim 7:

Wasilewski discloses "The method of claim 1 further comprising: decrypting the first

data stream at the set-top box; and decrypting the second data stream at the set-top

box" on (Page 34 lines 23-33, and Fig 15).

10. As per claim 8:

Wasilewski discloses, "The method of claim 1 and further comprising storing a portion of

the first set of encryption data in a RAM" in (page 34 lines 10-15).

11.   As per claim 9:

Wasilewski discloses "The method of claim 1 end further comprising storing a portion of

the first set of encryption data in a register of a microprocessor" on (page 25-28).

12.   As per claim 14:

Wasilewski discloses "A method of allocating resources comprising:

allocating a memory with a first set of decryption data corresponding to a first -

level-of-encryption;

receiving via from an originating source a first data stream having the first

level-of-encryption and a first number of services" on (Page 34 line 33 to Page 35 line

10);

"re-allocating the memory with a second set of decryption data corresponding to

a second-level-of-encryption the second-level-of-encryption the second-level-of-

encryption being different from the first-level-of-encryption the second-level-of-

encryption being different from the first-level-of-encryption of the first data stream;

receiving from the originating source a second data stream having the second-

level-of-encryption and a second number of services different from the first number of

services" on (Page 22 line 26 to Page 23 line14, and Page 26 lines 1-10) {The seeds

used to encrypt the number of services are changed every cryptocycle. Since new

seeds created for encryption of new number of services, the first level of encryption is

different from the second level of encryption. (See Page 23 lines 1-15)}; and

storing in memory said first set of decryption data corresponding to a first level of

encryption and second set of decryption data corresponding to said second level of

encryption" on (Page 35 lines 1-10).

13.   As per claim 15:

Wasilewski discloses "The method of claim 14 and further comprising detecting that the

second-level-of-encryption of the second data stream is different from the

first-level-of-encryption of the first data stream" on (Page 34 lines 25-33).

14.   As per claims 16 and 17:

Wasilewski discloses "the method as described in claim 14 wherein said allocating a

memory with a first set of decryption data corresponding to said first-level-of-encryption

comprises storing decryption key data; said memory with a second set of decryption

data corresponding to said second-level-of encryption comprises storing decryption key

data" on (Page 34 lines 25-33).

15.   As per claim 26:

Wasilewski discloses "The method of claim 24 wherein the second set of decryption

data comprises at least one decryption key" on (Page 34 lines 25-33).

Claim Rejections - 35 USC § 103

16.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

17.   Claims 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Wasilewski in view of Milsted et al, US Patent No 6263313, hereinafter "Milsted". (Cited

in US PTO 892 dated 08/11/05).

18.   As per claims 4 and 6:

Wasilewski only discloses "The method in claim 1 wherein said first-level of encryption

utilizes the Data Encryption Standard" in (Wasilewski, Col 9 lines 8-15), said

second-level-of encryption utilizes an encryption method uniquely separate from the

first.

However, Wasilewski does not teach of utilizes an algorithm different from said

Data Encryption Standard which is used in the first-level-of encryption.

Nevertheless, Milsted does teach of utilization of multiple encryption method in

protection of digital content before delivery in (Milsted, Col 15 lines 34-45).

Therefore, it would have been obvious at the time of the invention was made for

one having ordinary skill in the art to modify Wasilewski's invention to incorporate

Milsted's implementation of different encryption algorithm to each digital content for

transmission to the set-top-box destination for usage. The implementation of different

encryption algorithm to encrypt each digital content for transmission provides a different

security level of protection to the data.

19.   Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Wasilewski in view of Grube et al, US Patent No 5602916, hereinafter "Grube".

20.   As per claim 23:

Wasilewski discloses "A method of providing encrypted data, method comprising:

        providing a first set of services comprised of a first number of services;

encrypting at least one of services from first set of services at a first level-of-encryption"

" on (Page 25 lines 32-35) {Video, and multiplexed Audio services};

        combining the first set of services into a first data stream" on (Page 26 lines 1-

10);

        transmitting said first data stream" on (Set-top decoder 260, Page 34 lines 23-

32);

        storing a first set of decryption keys associated with said first-level-of-encryption,

said first set of keys corresponding to the decryption algorithm for the

first-level-of-encryption" on (Page 34 line 33 to Page 35 line 10);

        "providing a second set of services comprised of a second number services

different from the first number of services;

        encrypting at least one of services from second set of services with an

encryption algorithm different from first-level-of-encryption" on (Page 22 line 26 to Page

23 line14, and Page 26 lines 1-10) {The seeds used to encrypt the number of services

are changed every cryptocycle. Since new seeds created for encryption of new number

of services, the first level of encryption is different from the second level of encryption.

(See Page 23 lines 1-15)};

combining the second set of services into a second data stream;

transmitting said second data stream" on (Set-top decoder 260, Page 34 lines

23-32); and

storing a second set of decryption keys associated with second-level-of-

encryption in integrated circuit in set-top box".

However, Wasilewski does not teach of implementing first-level of encryption

algorithm and second-level-of encryption algorithm in encrypting and decrypting the

number of services.

Neverthless, Grube discloses the "Method and Apparatus For Preventing

Unauthorized Monitoring of Wireless Data Transmissions" invention, which includes a

method of encrypting a first request data for transmission at a first encryption level and

encrypting a second request data for transmission at a second encryption level (See

Figure 3, # 308, Col 5 lines 25-45). The receiving end (Figure 2, Col 4 lines 22-45) has

the algorithms and keys necessary to decrypt the received encrypted request data.

Therefore, it would have been obvious at the time of the invention was made for

one having ordinary skill in the art to modify Wasilewski's invention to incorporate

Grube's teaching of implementing different encryption algorithm to encrypt the data with

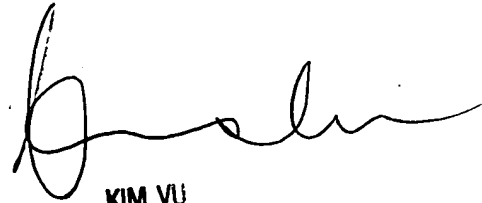the motivation of better secure the encryption for data transmission.

21.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Linh LD Son whose telephone number is 571-

272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PAT
TECHNOLOGY CENTER 2100